EXHIBIT B

How Much is Privacy Worth Around the World and Across Platforms?

Jeffrey Prince and Scott Wallsten*

March 2022

Abstract

Using carefully designed discrete choice surveys, we measure individuals' valuation of online privacy across countries (United States, Mexico, Brazil, Colombia, Argentina, and Germany) and data types (personal information on finances, biometrics, location, networks, communications, and web browsing). We find that Germans value privacy more than do people in the U.S. and Latin American countries. Across countries, people most value privacy for financial (bank balance) and biometric (fingerprint) information. People had to be paid the least for permission to receive ads – respondents in Argentina, Colombia and Mexico would even *pay* for them – followed by location privacy. We discuss privacy policy implications.

* Jeffrey Prince is at Indiana University, Department of Business Economics and Public Policy, Kelley School of Business. Scott Wallsten is President and Senior Fellow at the Technology Policy Institute. We thank the InterAmerican Development Bank for financial support, several focus groups for their time and insight, ResearchNow for assistance in administering the surveys, Phil Keefer and María Carmen for comments and suggestions, Lindsay Poss for research assistance, and Camila Rodriguez Gomes and Daniel Jaramillo for translation assistance. We are responsible for all errors. Any opinions expressed here are those of the authors and do not necessarily reflect the views of the Technology Policy Institute, its staff, or its board, or those of the IADB or anyone affiliated with it.

1. Introduction

The prevalence and value of data in virtually all sectors has grown tremendously, with some even declaring it the world's most valuable resource (Economist, 2017). However, along with this growth in volume and value has come increased importance in getting policy right—balancing privacy preferences with benefits that derive from the use of data. Such cost benefit analyses are currently difficult, if not impossible, due to the lack of market data that reveal how much people truly value different elements of privacy or the services they receive in exchange for use of that data. Indeed, the prevalence of nonmarket goods and services in the digital economy is a major obstacle to coherent policymaking. Nevertheless, issues ranging from high-profile data breaches (e.g., Equifax, 2017) and Facebook's Cambridge Analytica scandal to a general unease about access to personal information have made data privacy a matter of increasing concern for governments and businesses around the globe. In fact, data privacy was the focus of the World Bank's 2021 World Development Report (World Bank, 2021).

Despite widespread agreement on the need for some kind of data privacy oversight, agreement on what that means remains elusive. Typical comparisons involve the United States vs. Europe and the State of California. As of this writing, the U.S. government is discussing legislation and regulation beyond its current policy of imposing punishments and consent decrees after finding that a firm has violated existing laws or user agreements. By contrast, Europe has implemented a comprehensive set of data privacy regulations known as the General Data Protection Regulation (GDPR). The State of California passed a law known as the California Consumer and Privacy Act (CCPA), which took effect on January 1, 2020. With the legal and regulatory landscape fragmented, it is not surprising that data practices by firms are similarly inconsistent. Several Latin American countries, including Brazil, Colombia, Mexico, and

Argentina also either have or are considering privacy rules.[1] Firms vary on how they deal with data privacy, and third parties distribute rankings of the best and worst firms for protecting data privacy (e.g., eWeek, 2017).

With much disagreement on best public and private practices, and much at stake, it is unfortunate and perhaps surprising that so little empirical evidence exists on how people value different elements of data privacy. The evidence that does exist is often qualitative in nature, focusing on opinions regarding data privacy in general but not quantifying this general opinion or any particular type(s) of data privacy. Most relevant to our analysis, very little existing empirical evidence is suitable for determining relative valuations of different types of data privacy, much less how those values differ across countries.

In this paper, we estimate how much people value a range of highly relevant aspects of privacy and how these values vary across countries, data types, and platforms. Understanding the value of privacy is necessary for conducting any analysis of proposed privacy policies, both public and private, as these values are a key component of policy benefits. Because any such regulations will come with costs, such an understanding about benefits can help to ensure that proposed rules do not cost more than consumers and constituents would themselves want imposed.

If privacy values differ across countries or regions, then acceptable rules and regulations may similarly differ across regions. At a high level, if, for example, we were to discover that Europeans value certain elements of their privacy more than the U.S., then a strict privacy regime like that created by GDPR might yield net benefits in Europe but not the U.S. While we have a general sense, based on its history of relevant laws, that Europeans place a higher value

[1] https://www.tmf-group.com/en/news-insights/articles/2019/april/data-privacy-laws-across-latin-america/

on data privacy than do U.S. residents, even that basic information is lacking for Latin American countries. Do Latin Americans value data privacy even more than do Europeans, or do they value it even less than U.S. residents? Do these preferences vary significantly across Latin American countries? The answers to these questions are crucial for generating coherent privacy policies that will yield the most benefits.

Similarly, if people value the privacy of different types of data differently, then policy should probably also treat them differently. For example, in this research we find that generally people value the privacy of their biometric (e.g., fingerprint) data more than they do their location data. Given such a relative valuation, rules governing how biometric data can be collected and used may generate additional consumer surplus while stricter rules on how location data is collected and used may not.

To measure how much consumers value different types of data privacy and ultimately conduct our comparisons, we employed a battery of discrete-choice surveys—a trusted approach demonstrated to be far more reliable than open-ended surveys. This approach is especially relevant for data privacy valuation, given it closely mimics the types of choices individuals can make in real markets for personal data[2] and policy proposals that would have firms pay consumers for data.[3] We constructed four different survey structures, centered respectively on the respondent's wireless carrier, financial institution, smartphone, and Facebook account. Across the four survey structures, we measure values for a range of data privacy types, including personal information on: finances, biometrics, location, networks, communications, and web

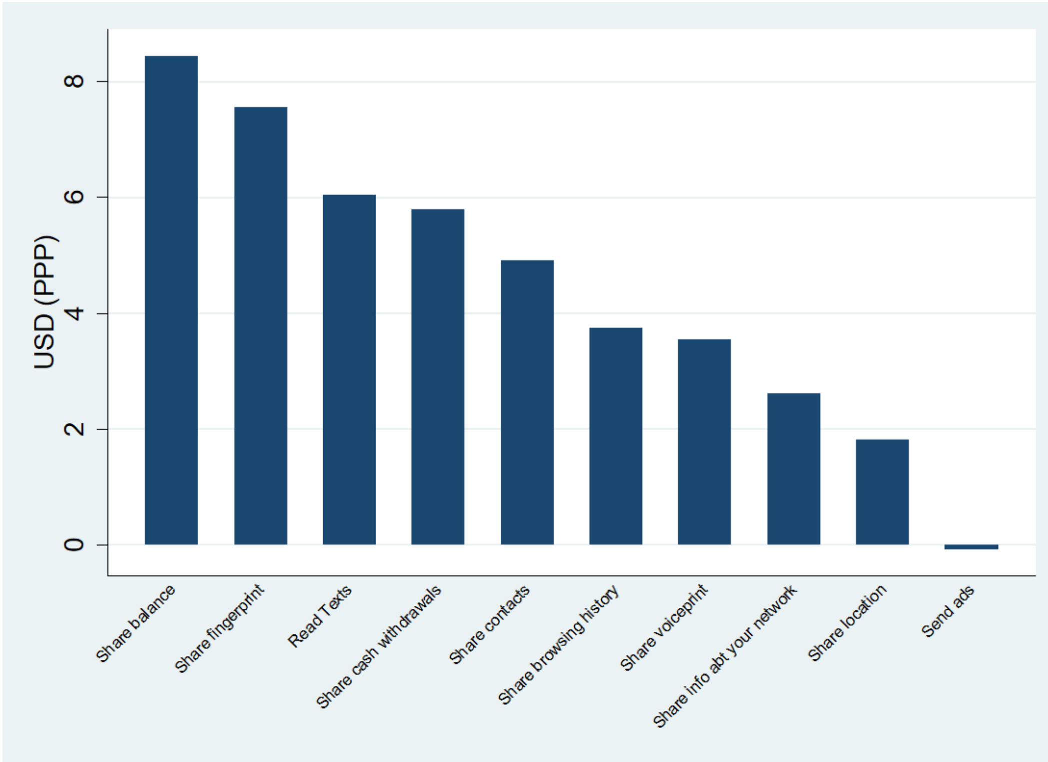
[2] For example, at the end of 2020, Amazon launched a program in which it would pay consumers to share information about non-Amazon purchases (https://techcrunch.com/2020/10/20/amazon-launches-a-program-to-pay-consumers-for-their-data-on-non-amazon-purchases/).
[3] California and other states have proposed requiring such payments (https://www.cnet.com/news/california-wants-silicon-valley-to-pay-you-a-data-dividend/).

browsing. We administered each of these four different surveys across six different countries: the United States, Mexico, Brazil, Colombia, Argentina, and Germany.

On average across countries and platforms, people placed the highest value on keeping financial data, biometric (fingerprint) information, and texts private, as shown in Figure 1. Specifically, to allow a platform to share this information with third parties, expressed in USD based on purchasing power parity (PPP) conversions, our surveys indicate that the platform would have to pay users $8.44/month to share a bank balance, $7.56/month to share fingerprint information, $6.05/month to read an individual's texts, and $5.80/month to share information on cash withdrawals. By contrast, people had to be paid only $1.82/month to share their location and essentially nothing to be sent ads via SMS.[4]

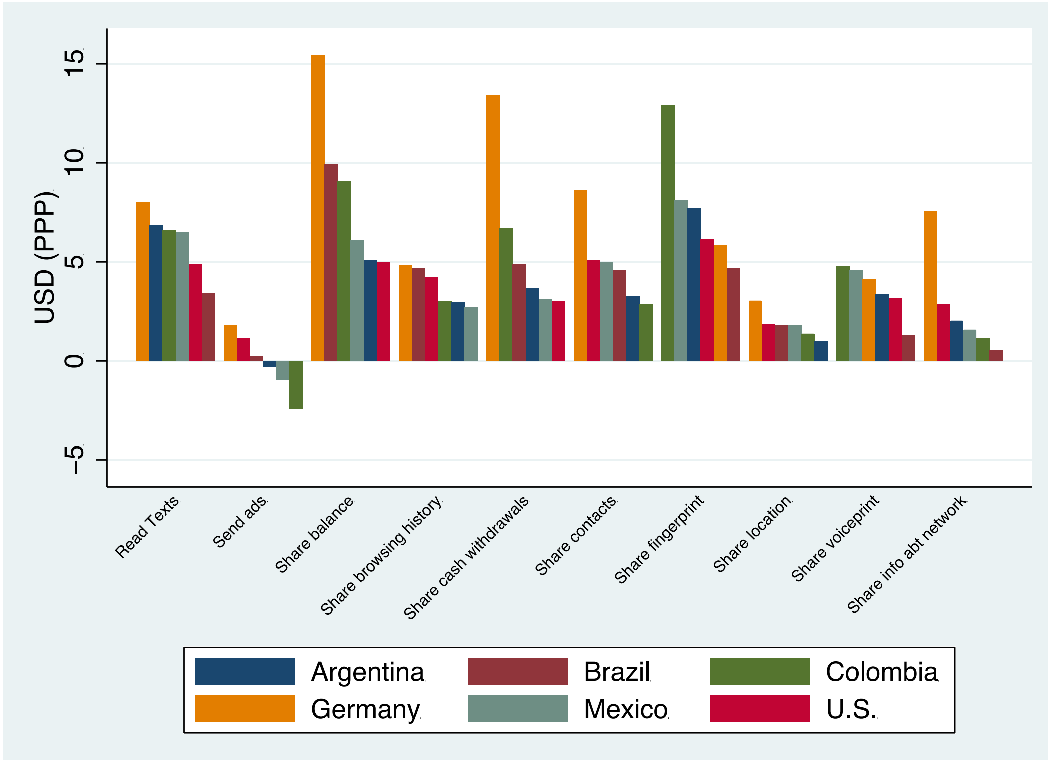
[4] These are estimates of willingness-to-accept (WTA).

Figure 1: Average Payment Consumers Would Demand for Permission to Share Data Across Countries and Platforms



These averages across data types mask significant differences across countries. In general, people in Germany valued privacy more than people in the U.S. and Latin America. Figure 2 contains the averages by country. This figure confirms what many believe, which is that Germans tend to value their privacy more than others. However, this summary finding is not true across the board and is particularly pointed for financial privacy. An example of an exception to Germans' relatively high privacy valuation is fingerprint information; on average, people across countries value fingerprint information the second highest in the list of data types we study, but Germans' value is well below that of several other countries. Another noteworthy result is not just that people value avoiding ads relatively little, but that people in Latin America seem to appreciate them—in Colombia, for example, people are willing to pay about $2.50/month to see ads.

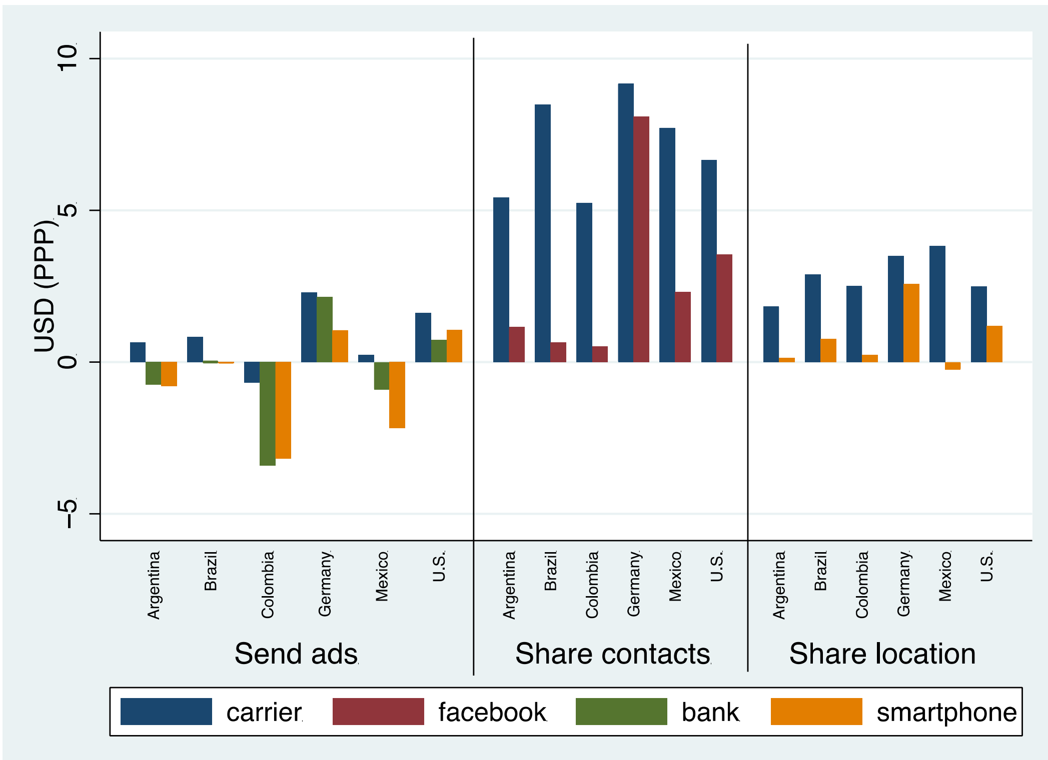
Figure 2: Average Payment Consumers Would Demand for Permission to Share Data Across Countries by Feature



We are also able to examine how values may differ across platform. In principle, if a user is giving an organization the right to share their data, then these values should not differ across platform since presumably each platform could share with the same third parties. In reality, though, people may have different levels of trust in different platforms or believe that data sharing practices differ. We do, in fact, see some differences across platforms for the same piece of data. The surveys did not ask about the same types of information for each platform, so our ability to compare across platforms is thus constrained. Figure 3 shows the available comparisons by platform and country. The figure shows that in all six countries, people must be paid more by their wireless carrier than other platforms to be sent ads, share contact information, and share location data. While people are more willing to share contact information with Facebook than with their wireless provider across countries, the amount Facebook would have to pay users for the right to share contact

information varies significantly across countries. Germany again shows its strong taste for privacy, with the U.S. in a distant second place; Facebook would need to pay German users about $8/month, Americans $3.50/month, to share their contact information. Across the Latin American countries, however, values are generally much lower: ranging from $2.30/month in Mexico to as little as $0.52/month in Colombia.

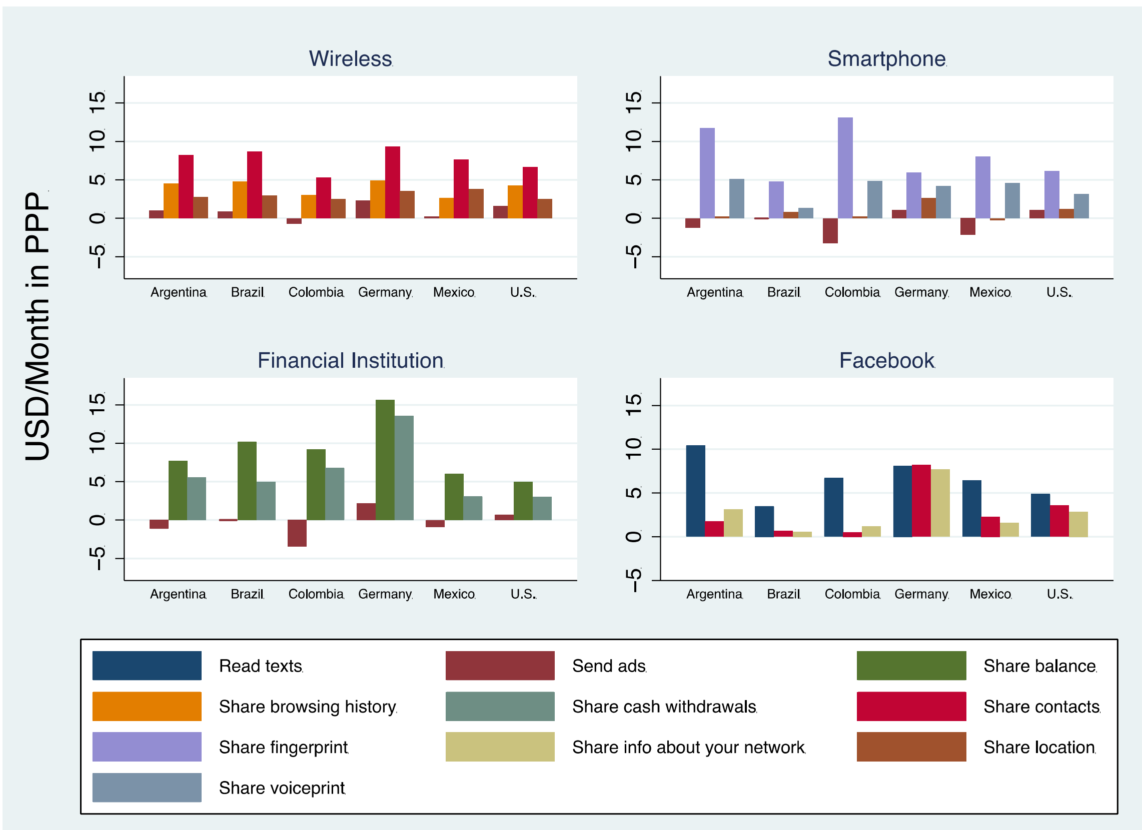
Figure 3: Average Payment Consumers Would Demand for Permission to Share Data Across Platforms and Countries



Overall (Figure 4), key international differences in relative rankings are most evident with regard to ads, with Latin Americans generally showing a preference for, rather than aversion to, ads on both their smartphone and from their financial institution – all in contrast to the U.S. and Germany. In absolute terms, we see consumers in all countries exhibiting relatively high values for privacy of financial information, with Germans having an especially high value. After accounting for Germany's high preference for financial privacy, we also see notable

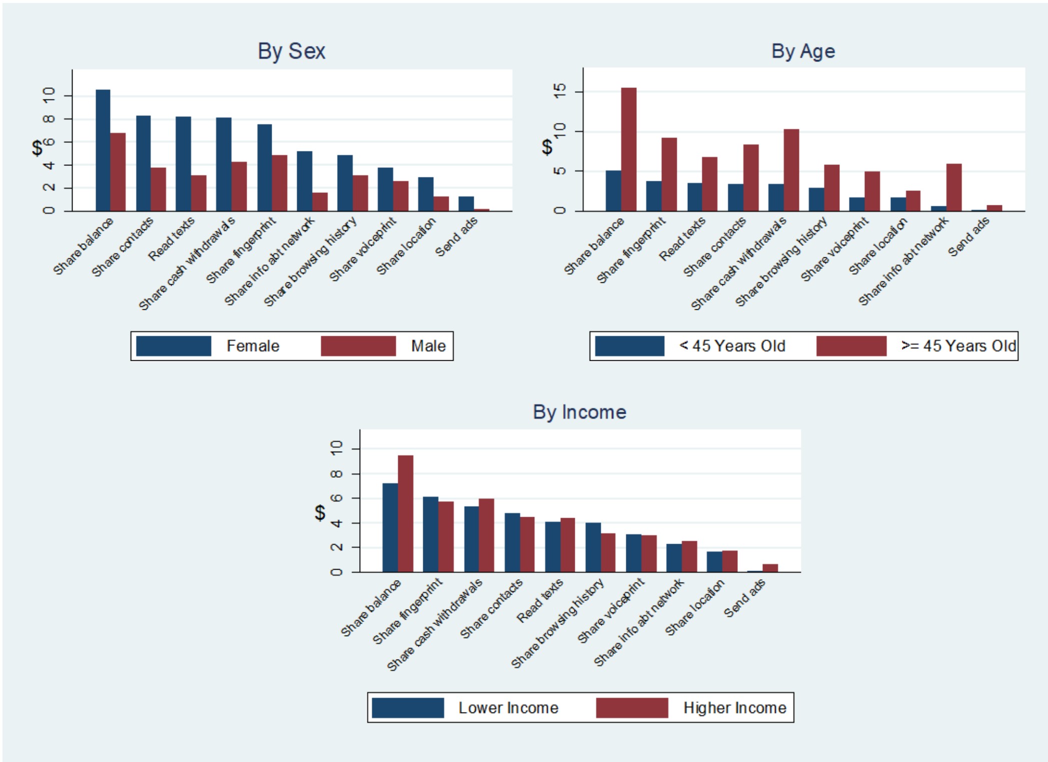
comparability in the magnitude and relative rankings in WTA for privacy across countries, with some exceptions (e.g., network information in Mexico and fingerprint information in Colombia). Additional analysis indicates that within-country variation in values is largely similar for each of the six countries, with Germans often exhibiting more homogeneous preferences compared to the others. We also observe positive correlations in privacy preferences across data types for individuals in all six countries.

Figure 4: Summary of Results



We also find consistent differences by sex in privacy valuations. Across platforms, data types, and countries, women value privacy more than men do. Similarly, older people value privacy more highly than younger people. We find no consistent differences in privacy valuations by income. Figure 5 shows these estimates averaged across platforms and countries.

Figure 5: Average Payment Consumers Would Demand for Permission to Share Data by Sex, Age, and Income



These results are largely robust to a randomly controlled treatment in the form of a leading statement about the value of data collection by these entities. Preferences for privacy are generally unaffected by such a prompt, suggesting that their values of online privacy are reasonably stable and not easily influenced.

Our findings have several implications. The striking consistencies in relative rankings of the value of online privacy across our six countries suggests that both public and private policies should probably offer similar *relative* privacy protections if facing similar costs and contexts for protection. However, differences in how much people value privacy of different data types across countries suggests that people in some places may prefer weaker rules while people in other places might prefer stronger rules. How much people value some data types does not vary

much across countries, however. In particular, people value the privacy of their contact information and texts fairly similarly across countries.

The generally similar within-country variation in values has interesting implications for both firms and governments. For firms, this suggests that, to the extent that tiered privacy protections may be economically sensible for one country, it may be economically sensible for all in our group. With respect to government policies, these results suggest that, when viewed in economic terms, the distribution of support for various protections is likely similar across countries. The notable exception in both cases is Germany, which appears to have more homogeneous preferences regarding online data privacy. Lastly, the positive correlation in individual-level privacy preferences across data types suggests that policies involving bundles of privacy types (e.g., protections for financial and biometric information) are unlikely to encounter more homogenized preferences (as might be possible if our correlations had been negative), potentially posing challenges in garnering widespread support.

2. The Value of Privacy

The empirical analysis in the paper measures the value of online privacy across different types of privacy, countries, and people within countries. In this section, we provide context for our empirics by discussing various existing methods for measuring the value of privacy, and determinants of such value.

2.1. Measuring the Value of Privacy

Measuring the value of data privacy can be challenging for myriad reasons. For starters, "privacy" in the abstract does not have a specific meaning. This problem is reminiscent of

challenges in valuing the environment, such as the value of having clean oceans or clean air. A solution is to quantify data privacy in general, such as the value of avoiding a major data breach. However, valuing something of this magnitude can be difficult, often relying on much-critiqued contingent valuation approaches.

A widely recognized phenomenon when it comes to data privacy is the so-called privacy paradox, where people say in surveys that they care a lot about privacy but behave as if they do not (e.g., Athey et al. 2017). For example, Savage and Waldman (2015) find high stated demand for privacy in apps; however, Kummer and Schulte (2019) show low revealed preference for app privacy. Rainie et al. (2013) note a 2013 Pew Research Center study that finds 68 percent of US adults believed current laws are insufficient in protecting individuals' online privacy, and Madden and Rainie (2015) find that 93 percent of U.S. adults believe that being in control of who can get information about them is important. Nevertheless, the results of the aforementioned measures for specific types of privacy indicate that the value of privacy notably varies with context and personal traits (Acquisti et al. 2015). Lastly, a recent study provides an international comparison of what is termed as the data confidence index (DCI), which measures expressed privacy concerns against stated online privacy behaviors (Datum Future & Global Web Index, 2019). They treat the DCI is a measure of the strength of the privacy paradox in a country, finding significant international variation.

A range of theories have been proposed to help explain the privacy paradox, ranging from differences between hypothetical and actual settings (Adjerid et al. 2018) to rational cost-benefit calculations (Barth and de Jong 2017 provide a review). Measurement of privacy preferences is further complicated by distinctions between willingness-to-pay (WTP) for privacy vs. willingness-to-accept (WTA) payment in exchange for disclosing otherwise private

information. A substantial literature finds that WTA estimates tend to be higher than WTP estimates, and that the two measures often have little correlation (See Chapman, et al. 2019 for a comprehensive discussion). Acquisti et al. (2013) specifically examines the difference between WTA and WTP for privacy in the context of linking a person's name to gift card purchases, finding a significantly higher WTA for linking the name compared to WTP to remain anonymous.

Contributing to our understanding of the privacy paradox and WTA-WTP differences, as well as privacy valuation in general, a range of prior studies (including the aforementioned) have attempted to measure individuals' monetary valuations for particular types of privacy, using a variety of approaches. These approaches include direct elicitation (e.g., Cvrcek et al. 2006), hypothetical auction (e.g., Huberman et al. 2005), field experiment (e.g., Acquisti et al. 2013), and discrete choice experiment (e.g., Savage and Waldman 2015). Additional studies have used surveys and other market data to generate measures for the value of privacy (e.g., Goldfarb and Tucker 2012). Earlier studies often focused attention on WTP analyses; however, perhaps driven by emerging markets for, and pricing by, information disclosure, more recent studies have tended to focus on WTA.[5]

Our analysis isn't designed to solve the privacy paradox or explain WTA-WTP gap, although it does add new data points for the privacy paradox discussion. Rather, our analysis builds off insights from prior work suggesting we might expect meaningful variation in the value of online privacy across different contexts, individuals, and even countries. Our analysis

[5] A non-exhaustive list of additional studies measuring privacy value includes: Tedeschi 2002, Wathieu and Friedman 2007, Savage and Waldman 2013, Hann et al. 2002, Tsai et al. 2011, Jentzsch et al. 2012, and Beresford et al. 2012.

examines and quantifies this type of variation for a set of highly relevant data types and platforms across several countries.

2.2. Determinants of the Value of Privacy

As noted above, prior work suggests context and personal traits are important determinants of the value of privacy. A particularly relevant component of personal traits includes cultural values, defined as a set of strongly held beliefs that guide attitudes and behavior and that tend to endure even when other differences between countries are eroded by changes in economics, politics, technology, and other external pressures (Hofstede 1980, Long & Quek 2002). Milberg et al. (2000) used a formative index to assess how four of Hofstede's (1980, 1991) cultural values indices – Power Distance Index (PDI), Individualism (IND), Masculinity (MAS), and Uncertainty Avoidance Index (UAI) – influence information privacy concerns. They found that concerns about information privacy were positively associated with PDI, IND, and MAS, and negatively associated with UAI. Hence, this prior work points to differences in general sentiment across countries but leaves open the question of whether and how such differences materialize for specific types of (online) privacy.

Conventional wisdom in conjunction with its legal history suggests Germans have particular concern about data privacy. Typical explanations for these preferences point to the country's relatively recent history with prevalent and dangerous surveillance.[6] Consequently, we might expect Germans to be more resistant to sharing personal data, leading us to expect higher

[6] For some examples of discussion on this topic, see: https://www.dotmagazine.online/issues/security/germany-land-of-data-protection-and-security-but-why and https://www.handelsblatt.com/english/handelsblatt-explains-why-germans-are-so-private-about-their-data/23572446.html?ticket=ST-4642680-KGub1dxIYWfSyZ11w535-ap2.

WTA in our surveys. Nonetheless, it is not clear whether we should expect these higher values to materialize across all data types or just among a subset.

3. Survey Design

The surveys we construct measure individuals' WTA to give up various forms of privacy, rather than their WTP to retain privacy. The choice to measure WTA rather than WTP is largely driven by the fact that several proposals and existing marketplaces, as described above, involve firms paying consumers for their data rather than consumers paying firms to keep their data private.[7] For this reason, we believe WTA is arguably the more appropriate measure relative to WTP.

To estimate WTA to give up various forms of privacy, we collect and analyze data from four separate surveys that employ repeated discrete choice experiments (DCEs). The four surveys pertain to respondents' wireless carrier, Facebook use, checking account at a bank, and smartphone. Because we are interested in comparing results across countries, the survey had to be in four languages given our country choices: English, Spanish, Portuguese, and German. We designed the survey in English, paid to have it translated into each language, and then had native speakers review the translations and compare to the English to ensure not just proper translation but also that the same meanings and information were conveyed to the respondent.

Prior work has shown that DCEs mitigate the reporting inaccuracy of stated-preference data (Carare et al. 2015). Even if hypothetical bias may potentially overestimate demand, the estimation for changes in feature levels is statistically unbiased, at least for WTP estimates (Ding

[7] As noted in Section 2, a substantial literature finds that WTA estimates tend to be higher than WTP estimates; this suggests that our estimates may be considered an upper bound.

et al. 2005; Miller et al. 2011).[8] A reliable DCE method, however, requires a careful design to cause respondents to answer truthfully, as if they are making a choice in the real market (Ben-Akiva et al. 2016). We thus structure the survey in three parts. We first collect relevant demographic information in order to conduct comparative analyses and to ensure a representative sample according to region, age, race, and sex. Demographics we collect include sex, age, proximity to a city, and household income.

The second part of the survey collects information regarding each respondent's current use of online services and connected devices that may collect personal information. We then provide respondents descriptions for each of the relevant features about which we will inquire in the third part of the survey. These descriptions are in the Appendix, and were carefully vetted by several focus groups.

Based on interactions with focus groups, we recognized many respondents may not be aware of how much data they are sharing currently. For example, some showed an initial aversion to sharing their voiceprint, until they were made aware that home devices like the Amazon Echo (via Alexa) and Google (via Assistant) may collect this information. We included examples in areas where lack of awareness of data sharing seemed particularly relevant.

The final part of the survey consists of repeated choice experiments. Here, we mimic the real market choice situation while exogenously varying our variables of interest – particularly, prices, exposure to ads, and the types of data the user shares. In the discrete choice experiments (DCEs), individuals make a series of choices over hypothetical alternatives, defined by a set of

[8] Specifically, Miller et al. (2011) attribute the upward bias to the non-incentive-aligned feature of the choice experiment. Participants do not need to actually pay for their choice in the hypothetical experiment and hence understate the possibility of choosing "none." The result is the biased demand intercept, but not the slope parameters, so WTP estimations remain valid in their test. In the context of Internet service, an incentive-aligned design is not possible due to high product cost, e.g. we cannot realistically offer a fiber-level service if no such infrastructure exists. On the other hand, we suspect that the Internet has become a necessity for most households, even at a reasonably high price. The tendency to choose "none" is likely to be low, especially given we are surveying current subscribers.

attributes. Since our primary goal is to estimate the WTA to give up specific elements of privacy, the core attributes are price and various measures of data privacy. We provide the descriptions and levels for each survey in Tables 1a-1d.

[Tables 1a-1d about here]

In principle, we could include other common attributes for each survey. However, our surveys are not designed to elicit choices over the products/services themselves (e.g., choices over different smartphones or checking accounts). Rather, for a given product or service, our respondents are asked to make choices about corresponding privacy packages. Such choices are not inconsistent with actual market decisions. For example, as mentioned earlier, Amazon has begun paying consumers for data about non-Amazon purchases, so markets for privacy already exist. We also note that the specific types of privacy we consider were generally motivated by existing policies, such as GDPR and CCPA.

Each respondent is presented with ten different choice questions, a common volume for such surveys at this level of complexity. In addition, to mitigate any endogeneity concern, we explicitly state that any omitted feature should be assumed to be identical across all alternatives. In other words, any omitted attributes are controlled for, i.e., held fixed, when making the comparison. If the survey involves a product or service already owned by the respondent, we specifically instruct them to treat all unmentioned features as being identical to the product or service they currently have.

Finally, for each of the four surveys, we randomize across two versions. The first is as described above. The second includes a statement at the top of the feature descriptions page, which

highlights the potential benefits of third-party data access, particularly with regard to targeted advertising. In our analysis, we examine whether the presence of such a statement materially impacts the value respondents indicate for their data privacy.

We provide the content of each survey (in English, i.e., the U.S. version) in the Appendix, including an example choice question and an indicator for the randomized statement concerning data value for advertising.

We conclude this subsection with a brief description of our process for arriving at an optimal design, i.e., the construction of the levels for each attribute presented to each respondent for each choice. For a statistically optimal design, we rely on D-optimality (Zwerina et al. 2010), which we implement in the statistical software program SAS. We use a fractional factorial design to capture the main effects.[9] Our relative D efficiency is 72.5%, 82.4%, 82.6%, and 72.4%, for the finance, smartphone, carrier, and Facebook surveys, respectively. The chosen design generates 150 choice questions for the smartphone and carrier surveys and 50 choice questions for the financial and Facebook surveys. The latter two have fewer features, and so require fewer variants. We grouped the choice questions into sets of ten (which we call versions), with four alternatives for the smartphone and carrier surveys and three alternatives for the financial and Facebook surveys. We randomly vary the alternatives for each choice, and randomly distribute the versions across respondents.

[9] We use SAS %mktruns and %mktex to produce candidate runs given our target sample size. We avoid dominated alternatives (i.e. better privacy and higher payment) by using the SAS %macro. We then evaluate and select the design by using SAS %choiceff.

4. Data

Our data come from ResearchNow's (RN)[10] standing Internet panel across six countries: Argentina, Brazil, Colombia, Germany, Mexico, and the United States. We requested 325 completed surveys per type (smartphone, etc.), per description header (information about data use for advertising or not), per country. Hence, our total number of requested completed surveys is 4*2*6*325 = 15,600. RN makes sure that the target sample sizes are satisfied. In our analysis, we also weight observations according to 2017 Census estimates for both age and sex[11].

A qualified response requires the household respondent to be at least 18 years old. For the carrier, Facebook, and smartphone surveys, respondents were required to have a carrier subscription, a Facebook account, or own a smartphone, respectively. In all three of these surveys, the respondent also must have been the primary decision-maker for the relevant product or service. For the financial survey, respondents were allowed to proceed even if they did not have a checking account.[12]

Appendix tables A1-A6 contain demographic distributions for each country, broken down by the four survey types.

5. Econometric Methods

To estimate values for privacy, we use a conditional logistic regression model (McFadden 1974; Greene 2012) to estimate utility parameters and ultimately calculate the WTA.

[10] Recently renamed "Dynata."
[11] We note that none of our qualitative findings depend on this weighting, and the quantitative findings only change minimally, suggesting any selection in terms of who completes the surveys in each country is unlikely to be driving our main results.
[12] Given the relatively large share of people without formal bank accounts in Latin America, we were concerned about excluding too many people with such a restriction and concluded that the questions were such that people could provide meaningful answers even if they did not currently have an account.

Let $\boldsymbol{x}_{ijk}$ be a vector of attributes for alternative *j* in choice question *k* that individual *i* faces. A linear random utility model can be written as:

$$u_{ijk} = \boldsymbol{x'}_{ijk}\boldsymbol{\beta} + \varepsilon_{ijk} \tag{1}$$

We interpret the errors (ε_{ijk}) as individual idiosyncratic preference and assume that it is independently and identically distributed with type I extreme value distributions. With this assumption the probability for individual *i* to choose alternative *j* among, say, four alternatives in question *k* is then

$$\text{Prob}(Y_{ik} = \text{j}) = \frac{\exp\,(\boldsymbol{x'}_{ijk}\boldsymbol{\beta})}{\sum_{n=1}^{4} \exp\,(\boldsymbol{x'}_{ink}\boldsymbol{\beta})} \tag{2}$$

Since we observe individual choices in each question, we are able to generate the likelihood function based on these probabilities. We then optimize the likelihood function with respect to $\boldsymbol{\beta}$ and obtain the estimated utility parameters for each attribute, clustering our errors on individuals.

The calculation of WTA for attributes relies on $\boldsymbol{\beta}$. In our case, the attributes include the personal data whose values we intend to estimate and the services the person would receive in exchange for providing that information. For illustration, consider our survey focusing on wireless carriers. In this survey, we partition $\boldsymbol{x'}_{ijk}$ into $[Price_{ijk}, Ads_{ijk}, Location_{ijk}, Browsing_{ijk}, Contacts_{ijk}]$, where each of the last four variables is a dummy variable equal to 1 if it is kept private and 0 otherwise. The corresponding $\boldsymbol{\beta'}$ is $[\beta_P, \beta_A, \beta_L, \beta_B, \beta_C]$. Using this formulation, the point estimate of WTA for giving up location data privacy, for example, can be monetized using the estimated β_P and β_L in the following formula:

$$WTA(share\ location) = -\frac{\beta_L}{\beta_P} \tag{3}$$

Finally, we estimate the variance of WTA by using a linear transformation of the variance-covariance matrix of $\boldsymbol{\beta}$, also known as the delta method.

A key merit of using a survey is the ability to generate sufficient variation in our variables of interest and cleanly identify the underlying parameters. The use of a hypothetical environment, however, may also induce unrealistic responses that generate bias. To minimize this possibility, we carefully designed our survey to elicit respondents' preferences and mimic the real market situation with respect to payments for data access. However, we are not actually collecting the private information we ask about (e.g., location data), nor are we providing an actual payment in return.

6. Results and Discussion

Tables A7-A10 contain our parameter estimates for all four surveys across all six countries. Tables 2a-2d then contain our valuation estimates, which we calculated as described in Section 5[13].

[Tables 2a-2d about here]

To facilitate comparisons, we convert each estimate into U.S. dollars using purchasing power parity (PPP) conversion rates provided by the International Monetary Fund for October

[13] Tables A11-A13 provide WTA comparisons across dichotomous breakdowns for sex, age, and income. These are preliminary findings that we intend to further explore in future research.

2019[14]. Although not a perfect means of comparison, it provides a clearer sense of relative valuations across countries.

Averaged across countries, people seemed most averse to sharing financial (particularly bank balance but also cash withdrawals) and biometric (fingerprint) information, and least averse to receiving ads and sharing their location (Table 3, last column). These results are sensible. Financial institution are often subject to specific privacy laws above and beyond those other institutions must follow.[15] Although regulatory governance of biometrics is not particularly common yet, some have expressed concerns about sharing biometric data due to the inability to replace identifiers like fingerprints or faces if the data are compromised.[16] On the other end, it is also sensible that people are not particularly averse to receiving ads. Ads are, at worst, a nuisance and can be helpful.

We find that people, on average required payments of about $9/month from their banks to for the right to share their balance and about $7.50/month from their smartphone manufacturer to share their fingerprint information. At the other end of the spectrum, people placed very low value on avoiding ads and required payments of $1.82/month for their location data. Interestingly, respondents were far less averse to sharing their voiceprint than their fingerprint, requiring nearly two times as much to share their fingerprint as their voiceprint. As shown below, this contrast is generally consistent across countries.

---

[14] https://www.imf.org/external/datamapper/PPPEX@WEO/OEMDC/ADVEC/WEOWORLD
[15] See, for example, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/financial-privacy
[16] See, for example, https://www.wired.com/2016/03/biometrics-coming-along-serious-security-concerns/

[Table 3 about here]

Across countries, Germans valued privacy more than people in the U.S. and Latin America, aligning with the widespread belief that Germans tend to value their privacy more than others.[17] However, we see in Table 3 that this basic insight is not true across the board and is most pronounced for financial privacy. For example, for fingerprint information – which has the second highest average value – Germany's value is well below that of several other countries. Notably, the U.S. and Latin American countries have similar values on average, and even similar to Germany outside of financial information. We also note that people in Latin America actually appear to appreciate ads—in Colombia, for example, people are willing to pay about $2.50/month to see ads. While we cannot tell the reason from the data, this could be due to differences in Latin American ads vs. Germany and the U.S. or differences in preferences for ads between Latin Americans compared to Germans and Americans. It could also be due to differences in assumptions made by each country's citizens about the prevalence of ad targeting. We note that marketing trends around the time of our study identify Latin America as a digital advertising hot spot.[18] The strong digital advertising presence in Latin America is consistent with relatively high digital ad preferences in that part of the world, providing some indirect corroboration of our result.

We also see variation across countries for each type of data and platform. Table 4 shows privacy values disaggregated across country, data type, and platform.

[17] See our discussion in Section 2.
[18] See, e.g., https://socialmediahq.com/why-digital-marketers-need-to-keep-an-eye-on-latin-america/. Digital advertising accounted for 40 percent of the ad market in Latin America by mid-2020.

[Table 4 about here]

For wireless carriers, we find a strikingly similar rank ordering of preferences across countries, with highest value for information on contacts, followed by browsing history, location, and ads. The range of values, however, is large and differs by country. Wireless providers in Germany would have to pay users $2.30/month for the right to send them ads by text while wireless providers in the U.S. would have to pay $1.63/month. In both countries, people would have to be paid four times by their wireless provider to allow the provider to share their contact information. While Germans generally place the highest value on information on contacts, browsing history, and location, it is by a relatively small margin, with notable similarity in magnitudes on the whole across countries.

We see the same international consistency in rank order for banks, with people placing higher values on checking balance compared to cash withdrawal information. Certain cross-country differences are stark for financial information. Germans stand out with high preference for privacy, requiring their banks to pay them $15.43 and $13.42 per month for the right to share information on their account balance and cash withdrawals, respectively. It is also notable that we see the starkest difference between Germany and the U.S. for banking information – the U.S. respondents place the lowest value on both types of banking information ($4.99 & $3.03), with the Latin American countries all somewhere in between, e.g., $3.30 for cash withdrawals in Mexico and $9.96 for balance in Brazil. The value people place on avoiding ads was much lower across all countries—over $2/month for Germany, about $0.75/month for the U.S., and generally negative for the Latin American countries.

Respondents are more averse to having Facebook read their texts read than to the platform sharing information about their networks or contacts. Germans seemed particularly averse to Facebook using their information in general, requiring the platform to pay them around $8/month for the right to read their texts or share information about their contacts or network. By contrast, people in the U.S. required about $5/month to allow access to their texts, $3.50 to share information about their contacts, and $3/month to share information about their networks. For Latin American countries, the numbers for texts are generally between those for the U.S. and Germany but lower than the U.S. for networks and contacts.

For smartphones, the rank ordering of privacy for different types of data is consistent internationally with, as might be expected, people valuing their biometric information far more than their location data or being sent ads. Latin Americans generally valued fingerprint data very highly, up to $12/month. Privacy preference for location data was the opposite, with Latin Americans placing quite low values, even negative in one case, on keeping that information private.

In sum, key international differences in relative rankings are most evident with regard to ads, with Latin Americans generally showing a preference for, rather than aversion to, ads on both their smartphone and from their financial institution – in contrast to the U.S. and Germany. In absolute terms, we see all countries exhibiting notable value for financial privacy, with Germany having an especially high value[19]. After accounting for Germany's high value for financial information, we also see notable comparability in the magnitude and relative rankings

[19] This finding provides an interesting complement to one of the findings in the 2019 report on the data confidence index (Datum Future & Global Web Index, 2019). In that report, the authors find Germany is least concerned about how companies use personal data or that the internet is eroding personal privacy, relative to the other countries in our sample. Combined with our results, this suggests that Germans believe their data to be well protected, but in the case that protection is not a given, are willing to pay the most to protect their data.

in value for privacy across countries, with some exceptions (e.g., network information in Mexico and fingerprint information in Colombia). Interestingly, this finding of general comparability implies that our Latin American countries (2/3rds of our sample), while (perhaps expectedly) comparable to each other in rankings and magnitude, are also quite similar to the U.S. and Germany on these dimensions, suggesting rather wide cross-cultural patterns in preferences. Lastly, for the two types of information we consider on multiple platforms (location and contacts), we see a notably higher values when it comes from the carrier than another source. While in principle ceding information privacy implies the same set of possibilities as to who ultimately will access it, this difference may imply distaste for the platform in general or more specifically a lower level of trust concerning what carriers will do with information they possess and can distribute.

We also collect demographic data about respondents, partly to ensure that the samples are representative, but also to allow us to make some comparisons across groups (see Tables A11 – A13). We find that women value privacy more than men do across privacy type, platform, and country without exception.

Additionally, older people generally value privacy more than younger people do. This finding is consistent with Goldfarb and Tucker (2012), who find that "Older people are much less likely to reveal information than are younger people." There are two exceptions to the age generality in our results. First, a few cases in which point estimates for older people are larger than for younger people but are not statistically significant. The lack of statistical significance exists for sending ads in Brazil, Colombia, and Mexico on wireless carriers and in Brazil for smartphones, although the magnitudes follow the same pattern as others. Second, in Argentina, young people value their financial privacy in terms of sharing their bank balance or information

on cash withdrawals more than old people, although the magnitude of the difference is small. In contrast to our findings on age, we find no consistent differences in privacy preferences across income.

In light of any lingering concerns about hypothetical bias or other data issues, we cross-check our findings with those of Milberg et al. (2000) along with current measures for the cultural metrics they use (PDI, IND, MAS, and UAI).[20] The key finding we attempt to cross-check is that, for occasions that one country has notably higher valuations for online privacy, that country is typically Germany. Further, by a small margin, the U.S. is second across all our measures. This finding generally aligns with the qualitative findings of Milberg et al. (2000). As noted in Section 2, they find that concerns about information privacy were positively associated with PDI, IND, and MAS, and negatively associated with UAI. Recent estimates for these cultural metrics indicate that Germany and the U.S. have the lowest scores (of the six countries) for UAI, and either the highest or near highest scores for IND and MAS, respectively. However, Germany and the U.S. have the lowest scores for PDI. Nonetheless, these measures are largely consistent with Germany and the U.S. having the highest WTA, particularly given Milberg et al. (2000) finds PDI to have the smallest impact on privacy concerns of the four cultural measures.

Beyond our international comparisons, we also consider within-country variation in valuation for online privacy. To do this, rather than estimate a fixed (mean) utility for each of the non-price variables in our surveys, we assume a normal distribution for each and estimate its mean and variance. This expanded approach allows us to estimate the level of heterogeneity in preferences for different types of online privacy for each country. The estimated coefficients are

[20] Recent estimates can be found at https://www.hofstede-insights.com/product/compare-countries/.

in Tables A14-A17. We report a simple measure of preference heterogeneity, the coefficient of variation (COV, which equals the standard deviation divided by the mean), for each type of online privacy for each country in Tables 5a-5d. Here we see that within country variation is largely similar for each of the six countries, with Germans often exhibiting notably more homogeneous preferences compared to the others. We also note that, in absolute terms, the COV roughly lies in the range of 1 to 3 for nearly all of our privacy measures. Particularly for the higher COV values, this suggests a significant proportion of individuals have WTA well above the mean while there is also likely a significant proportion with WTA near zero (assuming it is never negative).

[Tables 5a-5d about here]

We considered several other ways to capture heterogeneity in preferences across individuals for the different countries.[21] First, we used kernel estimators to trace out posterior distributions for our privacy preference parameters, conditional on the choice sets and choices made. Most posteriors roughly match the assumed normal distribution from the random coefficients model, while a minority exhibited some level of bimodality.[22] We also considered ways to capture whether and how privacy preferences are correlated within individuals across different types of privacy. To do this, we estimated our random coefficients model allowing for correlated coefficients (estimates are again in Tables A14-A17). Our results universally point to positive correlations for privacy preferences. We corroborated this finding by conducting latent

[21] Due to the sheer volume of analyses, we do not include the posterior distributions or latent class results. However, they are all available upon request.
[22] Lin (2019) also finds bimodality in some estimated privacy preferences. Further analysis in that study suggests that their bimodalities are driven by differences in racial preferences. Lacking a measure for race in our data, we cannot assess whether it is driving our findings; nonetheless, our finding of bimodalities for some of our privacy preferences suggests that Lin's findings of bimodality are more generally prevalent.

class analysis, allowing for latent class sizes between 3 and 5. Within-class correlations are universally positive for our various types of privacy.

Lastly, Tables 6a-6d present differences in values for each type of online privacy between the survey that highlights the potential benefits of third-party data access and the one that doesn't. Here, we generally see little difference between the two survey versions. While a few coefficients indicate some statistical significance, there is not a clear pattern. Further, Holm adjusted p-values and joint tests of significance indicate failure to reject the differences as zero. Hence, it appears that preferences for privacy are generally unaffected by prompts indicating potential benefits from sharing online personal information. We contrast this finding with an earlier Pubmatic study,[23] which found a significant difference in attitudes toward Internet advertising depending on respondents' understanding of the anonymity of their data, where attitudes were more positive when told their data remains anonymous. Together, our studies suggest that an alert that anonymity will be preserved is more impactful than one about potential benefits of data sharing.

[Tables 6a-6d about here]

Because of our unique focus on specific platforms and types of data across countries, few other results exist to compare against our own. One exception is Savage and Waldman (2013), discussed earlier, who focus on WTP for privacy in smartphone apps, as opposed to our WTA approach. Among other types of data, they investigated how much people were WTP to keep their location hidden from smartphone apps. They found that people were WTP $1.19 to keep location hidden. While we do not ask about smartphone apps explicitly, we explore how much people are

[23] https://www.mediapost.com/publications/article/145720/pubmatic-consumers-confused-about-online-tracking.html

WTA to allow their smartphone to share their location. We estimate a WTA of $1.20 in the U.S. for smartphones, remarkably close to their $1.19, providing some element of external validity.

Other comparisons are less clean, as we focus on other platforms while Savage and Waldman focus on apps. They estimate WTP $4.05 to conceal contact information from apps while we estimate WTA $5.11 averaged across Facebook and wireless carrier (the two platforms on which we include this data type), which seem reasonably similar. Finally, they estimate a WTP of $2.12 to eliminate advertising in apps, while we estimate WTA of $1.06 in the U.S. to allow your smartphone to send ads. Whether the difference is due to changes in attitudes about ads over time, different valuations of in-app advertising versus receiving ads on your smartphone more generally, or something else, we cannot say.

A natural question is whether the results are additive—that is, is it meaningful to add the data types within a platform and conclude that the sum is a total value for all those data types combined? In short, the answer largely depends on the degree to which preferences for different types of data privacy are interrelated. We did not explore any interactions in this exercise, given the already-substantial complexity of the survey instruments. It remains work for future research.

7. Conclusions

Our findings have several implications. The striking consistencies in relative rankings of the value of online privacy across our six countries suggests that both public and private policies should offer similar *relative* privacy protections if facing similar costs and contexts for protection. However, when it comes to advertisements, and some other specific examples such as financial information for Germany, notable discrepancies between Latin America, Europe, and the U.S. should be considered and could provide a basis for different protection policies generally or at the

sectoral level. Germany stands out as placing the highest value on privacy, driven by their strong preference for financial privacy. After controlling for this difference, we see largely similar valuations across all six countries (with some notable exceptions). This finding suggests stricter protections such as those in GDPR may be relatively more sensible for Europe, but there may be a case for largely similar protections – be they strict or lax – across all these countries.

The largely similar within-country variation in values that we find has interesting implications for both firms and governments. For firms, this finding suggests that, to the extent tiered privacy protections may be economically sensible for one country, it is likely economically sensible for all in our group depending on costs and contexts. With respect to government policies, these results suggest that, when viewed in economic terms, the distribution of support for various protections is likely similar across countries. The notable exception in both cases is Germany, which appears to have more homogeneous preferences regarding online data privacy. Lastly, the positive correlation in individual-level privacy preferences across data types suggests that policies involving bundles of privacy types (e.g., protections for financial and biometric information) are unlikely to encounter more homogenized preferences (as might be possible if our correlations had been negative), potentially posing challenges in garnering widespread support.[24]

Finally, the absence of any notable change in estimated value when respondents are prompted about possible benefits from sharing information suggests that their values of online privacy are reasonably stable and not easily influenced.

Proposed and enacted privacy regulations have not included cost benefit analyses, leaving assessments of their welfare impacts open to a wide range of interpretations, often depending on

---

[24] This point essentially stems from the fact that $Var(X + Y) = Var(X) + Var(Y) + 2Cov(X,Y)$. Hence, positive covariance tends to exacerbate the spread while negative covariance tends to mitigate the spread in preferences.

one's theory behind the commonly studied privacy paradox. The research discussed in this paper is one approach toward assessing some of the benefits that might be obtained from privacy regulations. As we have highlighted throughout this paper, the findings can particularly illuminate relative evaluations in addition to providing some useful insights about the value of keeping all manner of data private. Beyond this, more complex work could explore how the different pieces of data interact. Nonetheless, any full accounting of privacy regulations requires estimates of their costs as well.

Our estimates therefore cannot, by themselves, uncover the net value of privacy. For example, suppose we fully relied on our estimates as measures of benefits of privacy protections. We estimate that in the U.S., on average, consumers value keeping location data at $1.20 per month on a smartphone. Suppose further that keeping location data private meant no or less accurate driving directions on the person's smartphone. The net benefits of requiring smartphones to keep location data private would, therefore, be $1.20 minus however much people value high-quality directions on their phones. The same argument is true for all types of data. In short, more research is necessary to do any full cost benefit analyses. Given the importance of data in the digital economy and the amount of data people share, it would seem prudent to continue this work.

References

Acquisti, A., Brandimarte, L., and Loewenstein, G. 2015. "Privacy and Human Behavior in the Age of Information." *Science*, 347, 509-514.

Acquisti, A., John, L. K., and Loewenstein, G.. 2013. "What is Privacy Worth?" *The Journal of Legal Studies*, 42, 249-274.

Acquisti, A., Taylor, C., and Wagman, L.. 2016. "The Economics of Privacy" *Journal of Economic Literature*, 54, 442-492.

Adjerid, I., Peer, E., and Acquisti, A. 2018. "Beyond the Privacy Paradox: Objective Versus Relative Risk in Privacy Decision Making." MIS Quarterly, 42, 2, 465-488.

Ahlfeldt, G, Koutroumpis, P., and Valletti, T.. 2016. "Speed 2.0: Evaluating Access to Universal Digital Highways." CEPR Discussion Paper 11046.

Athey, S., Catalini, C., and Tucker, C. 2017. "The Digital Privacy Paradox: Small Money, Small Costs, Small Talk." NBER working paper.

Barth, S. and de Jong, M. 2017. "The Privacy Paradox – Investigating Discrepancies between Expressed Privacy Concerns and Actual Online Behavior – A Systematic Literature Review." *Telematics and Informatics*, 34, 7, 1038-1058.

Bellman, S., Johnson, E., Kobrin, S., and Lohse, G.. 2004. "International Differences in Information Privacy Concerns: A Global Survey of Consumers." *The Information Society*, 20, 313-324.

Ben-Akiva, M., McFadden, D., and Train, K.. 2016. "Foundation of Stated Preference Elicitation: Consumer Behavior and Choice-Based Conjoint Analysis." Working paper.

Beresford, A., Kubler, D., and Preibusch, A. 2012. "Unwillingness to Pay for Privacy: A Field Experiment." *Economics Letters*, 117, 25-27.

Bhagat, N. 2014. "Estimating the Value of Online Smartphone Privacy." Dissertation Thesis, University of Colorado, Boulder.

Carare, O., McGovern, C., Noriega, R., and Schwarz, J.. 2015. "The Willingness to Pay for Broadband of Non-Adopters in the U.S.: Estimates from a Multi-State Survey." *Information Economics and Policy*, 30, 19-35

Caussade, S., de Dios Ortúzar, J., Rizzi, L. I., and Hensher, D., 2005. "Assessing the Influence of Design Dimensions on Stated Choice Experiment Estimates." *Transportation Research Part B*, 39(7):621-640.

Chapman, J., Dean, M., Ortoleva, P., Snowberg, E., Camerer, C., 2019. "Willingness to Pay and Willingness to Accept are Probably Less Correlated Than You Think." Working Paper. http://www.columbia.edu/~md3405/Working_Paper_22.pdf

Christin, D., Buchner, C., and Leibecke, N. 2013. "What's the Value of Your Privacy? Exploring Factors That Influence Privacy-Sensitive Contributions to Participatory Sensing Applications." *38th Annual IEEE Conference on Local Computer Networks – Workshops*.

Cvrcek, D. Kumpost, M., Matyas, V., and Danezis, G. 2006. "A Study on the Value of Location Privacy." *Proceedings of the 5th ACM Workshop on Privacy in Electronic Society*.

Czajkowski, M., Giergiczny, M., and Zawojska, E.. 2015. "Does the Number of Discrete Choice Alternatives Matter for Respondents' Stated Preferences? The Case of Tap Water Quality Improvement." Working Paper.

Datum Future & Global Web Index. 2019. "The Data Confidence Index," https://www.datumfuture.org/wp-content/uploads/2019/09/Data-Confidence-Index-Datum-Future-and-GWI-2019.pdf.

Ding, M., Grewal, R., and Liechty, J.. 2005. "Incentive-Aligned Conjoint Analysis," *Journal of Marketing Research*, 42, 67–82.

Economist. 2017. "The World's Most Valuable Resource Is No Longer Oil, But Data."

EWeek. 2017. "The Best and Worst Companies for Defending Your Data Privacy."

Greene, W. H. 2012. Econometric Analysis. 7th ed. Upper Saddle River, NJ: Prentice Hall.

Goldfarb, A. and Tucker, C. 2012. "Shifts in Privacy Concerns." *American Economic Review*, 102(3), 349-353.

Hann, I. Hui, K., Lee, T., and Png. I. 2002a. "Online Information Privacy: Measuring the Cost-Benefit Trade-Off." 6th *ICIS*.

Hofstede, G. 1980. Culture's Consequences: International Differences in Work-Related Values. Sage Publications, Beverly Hills, CA.

Hofstede, G. 1991. Cultures and Organizations. McGraw-Hill, Berkshire, England.

Hofstede Insights, https://www.hofstede-insights.com/product/compare-countries, accessed November 6, 2019.

Huberman, B., Adar, E., and Fine, L. 2005. "Valuing Privacy." *IEEE Security & Privacy*, 3, 22-25.

Hugl, U. 2011. "Reviewing Person's Value of Privacy of Online Social Networking." *Internet Research*, 21, 384-407.

Hui, K., Teo, H., and Lee, S. 2007. "The Value of Privacy Assurance: An Exploratory Field Experiment." *MIS Quarterly*, 31, 19-33.

Jentzsch, N., Preibusch, S., and Harasser, A. 2012. "Study on Monetising Privacy: An Economic Model for Pricing Personal Information." ENISA.

Johnson, G.A., Shriver, S.K., and Du, S. 2020. "Consumer Privacy Choice in Online Advertising: Who Opts Out and at What Cost to Industry?" *Marketing Science*, 39(1), 33-51.

Kamakura, W.A. and Russell, G.J. 1989. "A Probabilistic Choice Model for Market Segmentation and Elasticity Structure." *Journal of Marketing Research*, 26(4), 379-390.

Krasnova, H., Hildebrand, T., and Oliver, G. 2009. "Investigating the Value of Privacy on Online Social Networks: Conjoint Analysis." *13th ICIS*.

Kummer, M. and Schulte, P. 2019. “When Private Information Settles the Bill: Money and Privacy in Google’s Market for Smartphone Applications.” *Management Science*, 65(8), 3470-3494.

Lin, T. 2019. “Valuing Intrinsic and Instrumental Preferences for Privacy.” Working paper.

Long, W. and Quek, M. 2002. “Personal Data Privacy Protection in an Age of Globalization: the US-EU Safe Harbor Compromise.” *Journal of European Public Policy*, 3, 325-344.

Madden, M. and Rainie, L. 2015. “Americans’ Attitudes about Privacy, Security, and Surveillance.” Pew Research.

McFadden, D. 1974. “Conditional Logit Analysis of Qualitative Choice Behavior.” In P. Zarembka, ed., *Frontiers in Econometrics*. New York: Academic Press.

Milberg, S.J., Smith, H.J., and Burke, S.J. 2000. “Information Privacy: Corporate Management and National Regulation.” *Organization Science* 11, 35–57.

Miller, K.M., Hofstetter, R., Krohmer, H., and Zhang, Z.J. 2011. “How Should Consumers’ Willingness to Pay Be Measured? An Empirical Comparison of State-of-the-Art Approaches.” *Journal of Marketing Research*, 48, 172-184.

Morningstar.com. 2019. Exchange rates for 9/2018-9/2019.

Png, I. 2007. “On the Value of Privacy from Telemarketing: Evidence from the ‘Do Not Call’ Registry.” Working Paper, National University of Singapore.

Rainie, L., Kiesler, S., Kang, R., and Madden, M. 2013. “Anonymity, Security, and Privacy Online.” Pew Research.

Savage, S. and D. Waldman. 2013. “The Value of Online Privacy.” Working Paper, University of Colorado.

Savage, S. and D. Waldman. 2015. “Privacy Tradeoffs in Smartphone Applications.” *Economics Letters*, 137, 171-175.

Savage, S., and D. Waldman. 2008. “Learning and Fatigue During Choice Experiment: A Comparison of Online and Mail Survey Modes.” *Journal of Applied Econometrics*, 23, 351-371.

Smith, H., Dinev, T., and Heng, X. 2011. “Information Privacy Research: An Interdisciplinary Review.” *MIS Quarterly*, 35, 989-1016.

Tang, H. 2019. “The Value of Privacy: Evidence from Online Borrowers.” Technical report, HEC Paris.

Taylor, C. 2004. “Consumer Privacy and the Market for Customer Information.” *RAND Journal of Economics*, 35, 631-650.

Tedeschi, B. 2002. "Everybody Talks about Online Privacy, but Few Do Anything about It." *New York Times*.

Tsai, J., Egelman, S., Cranor, L., and Acquisti, A. 2011. "The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study." *Information Systems Research*, 22, 254-268.

Wathieu, L and Friedman, A.. 2007. "An Empirical Approach to Understanding Online Privacy." Harvard Business School Research Paper.

World Bank. 2021. "Data for Better Lives," 2021 World Development Report. file:///C:/Users/jeffprin/Dropbox/PC/Downloads/9781464816000.pdf

Zwerina, K., Huber, J., and Kuhfeld, W.F. 2010. "A General Method for Constructing Efficient Choice Designs," *Marketing Research Method in SAS*, SAS Institute Inc., Cary, NC, USA.

Tables

Table 1a: Attributes, Descriptions, and Levels for Carrier Survey

Attributes	**Descriptions and Levels**	**Levels**
Monthly Payment	The amount you would receive in monthly payments from the carrier. This payment to you is separate from the price you pay for your wireless plan	Arg:\$0, \$10, \$20,…,\$160, \$170 Bra.:\$0,\$1,…\$8,\$8.50,\$9,\$10,…\$15,\$16 Col.:\$0,\$750,\$1500,…,\$12,000,\$12,750 Ger:€0,€0.25,€0.50,…,€4.00,€4.25 Mex:\$0,\$5,\$10,…,\$80,\$85 U.S.:\$0,\$0.25,\$0.50,…,\$4.00,\$4.25
Sends Ads	The carrier is able to send ads to your smartphone via text message	No or Yes
Shares Location	The carrier can use and distribute your location information to any company or individual that pays for it	No or Yes
Shares Browsing History	The carrier can use and distribute your browsing history to any company or individual that pays for it	No or Yes
Shares Contact List	The carrier can use and distribute your contact list to any company or individual that pays for it	No or Yes

Table 1b: Attributes, Descriptions, and Levels for Financial Survey

Attributes	**Descriptions and Levels**	**Levels**
Monthly Payment	The amount you would receive in monthly payments from the bank.	Arg:$0, $10, $20,…,$160, $170 Bra.:$0,$1,…$8,$8.50,$9,$10,…$15,$16 Col.:$0,$750,$1500,…,$12,000,$12,750 Ger:€0,€0.25,€0.50,…,€4.00,€4.25 Mex:$0,$5,$10,…,$80,$85 U.S.:$0,$0.25,$0.50,…,$4.00,$4.25
Sends Ads	The bank is able to send ads to your smartphone via text message	No or Yes
Shares Balance	The bank can use and distribute your balance information to any company or individual that pays for it	No or Yes
Shares Frequency and Amounts of Cash Withdrawals	The bank can use and distribute information about the frequency and amounts of your cash withdrawals to any company or individual that pays for it	No or Yes

Table 1c: Attributes, Descriptions, and Levels for Smartphone Survey

Attributes	**Descriptions and Levels**	**Levels**
Monthly Payment	The amount you would receive in monthly payments by a third party.	Arg:$0, $10, $20,…,$160, $170 Bra.:$0,$1,…$8,$8.50,$9,$10,…$15,$16 Col.:$0,$750,$1500,…,$12,000,$12,750 Ger:€0,€0.25,€0.50,…,€4.00,€4.25 Mex:$0,$5,$10,…,$80,$85 U.S.:$0,$0.25,$0.50,…,$4.00,$4.25
Sends Ads	The third party is able to send ads to your smartphone via text message	No or Yes
Shares Fingerprint	The third party can use and distribute your fingerprint information to any company or individual that pays for it	No or Yes
Shares Voiceprint	A voiceprint is the data required for a computer to identify your voice as yours. For example, Alexa on an Amazon Echo can use this information to identify you as the speaker. The third party can use and distribute your voiceprint information to any company or individual that pays for it	No or Yes
Records Location	The third party can use and distribute your location information to any company or individual that pays for it	No or Yes

Table 1d: Attributes, Descriptions, and Levels for Facebook Survey

Attributes	**Descriptions and Levels**	**Levels**
Monthly Payment	The amount you would receive in monthly payments by a third party.	Arg:$0, $10, $20,…,$160, $170 Bra.:$0,$1,…$8,$8.50,$9,$10,…$15,$16 Col.:$0,$750,$1500,…,$12,000,$12,750 Ger:€0,€0.25,€0.50,…,€4.00,€4.25 Mex:$0,$5,$10,…,$80,$85 U.S.:$0,$0.25,$0.50,…,$4.00,$4.25
Reads Texts	Facebook can use and distribute information from your texts to any company or individual that pays for it. Note that this includes texts sent using WhatsApp and Facebook Messenger.	No or Yes
Uses Network	Facebook can use and distribute information about your friend network to any company or individual that pays for it.	No or Yes
Access Contacts	Facebook can use and distribute your contact list from your smartphone to any company or individual that pays for it.	No or Yes

Table 2a: WTA Estimates for Carrier Survey

	Argentina	Brazil	Colombia	Germany	Mexico	U.S.
Send Ads	15.60** (6.13)	1.74 (1.54)	-913.07* (455.44)	1.77** (0.31)	2.13 (3.18)	1.63** (0.40)
Share location	43.91** (7.36)	6.00** (1.65)	3364.05** (604.74)	2.70** (0.44)	35.71** (4.81)	2.50** (0.51)
Share contacts	129.66** (14.12)	17.67** (3.30)	7035.25** (922.81)	7.07** (0.86)	71.88** (7.55)	6.66** (1.13)
Share browsing history	71.51** (9.30)	9.72** (2.24)	4033.31** (744.15)	3.73** (0.50)	25.17** (3.99)	4.25** (0.76)

Units are in each country's currency. Standard errors in parentheses. + is significant at 10% level. * is significant at 5% level. ** is significant at 1% level.

Table 2b: WTA Estimates for Financial Survey

	Argentina	Brazil	Colombia	Germany	Mexico	U.S.
Send ads	-17.78* (7.05)	0.01 (1.28)	-4571.51** (1106.67)	1.65** (0.43)	-8.39+ (4.43)	0.73** (0.25)
Share balance	121.45** (13.71)	20.72** (4.15)	12181.23** (2440.85)	11.88** (1.98)	56.82** (8.80)	4.99** (0.79)
Share cash withdrawals	87.53** (11.73)	10.14** (2.42)	9004.59** (1806.81)	10.33** (1.77)	29.04** (6.03)	3.03** (0.53)

Units are in each country's currency. Standard errors in parentheses. + is significant at 10% level. * is significant at 5% level. ** is significant at 1% level.

Table 2c: WTA Estimates for Smartphone Survey

	Argentina	Brazil	Colombia	Germany	Mexico	U.S.
Send Ads	-18.87** (7.12)	-0.08 (0.62)	-4269.86** (871.46)	0.81** (0.26)	-20.27** (3.70)	1.06** (0.28)
Share location	3.46 (7.68)	1.61* (0.81)	329.76 (835.74)	1.99** (0.31)	-2.26 (3.87)	1.20** (0.32)
Share fingerprint	184.25** (20.35)	9.73** (1.37)	17290.30** (2186.27)	4.51** (0.59)	75.51** (9.09)	6.13** (0.88)
Share voiceprint	80.56** (11.39)	2.75** (0.86)	6400.68** (1185.91)	3.17** (0.45)	42.84** (6.20)	3.18** (0.52)

Units are in each country's currency. Standard errors in parentheses. + is significant at 10% level. * is significant at 5% level. ** is significant at 1% level.

Table 2d: WTA Estimates for Facebook Survey

	Argentina	Brazil	Colombia	Germany	Mexico	U.S.
Read Texts	164.13** (16.62)	7.09** (1.04)	8851.95** (868.91)	6.17** (1.45)	60.51** (6.78)	4.91** (0.84)
Shares information about your network	48.72** (8.44)	1.16** (0.41)	1531.76** (464.39)	5.83** (1.47)	14.73** (3.33)	2.87** (0.58)
Share contacts	27.90** (7.16)	1.36* (0.62)	693.66+ (410.76)	6.23** (1.46)	21.45** (4.11)	3.55** (0.67)

Units are in each country's currency. Standard errors in parentheses. + is significant at 10% level. * is significant at 5% level. ** is significant at 1% level.

Table 3: Average WTA By Feature Across Country and Platform

	Argentina	Brazil	Colombia	Mexico	Germany	U.S.	Average
Share balance	5.08	9.96	9.09	6.10	15.43	4.99	8.44
Share fingerprint	7.71	4.68	12.90	8.11	5.86	6.13	7.56
Read texts	6.86	3.41	6.61	6.50	8.01	4.91	6.05
Share cash withdrawals	3.66	4.88	6.72	3.12	13.42	3.03	5.80
Share contacts	3.29	4.57	2.88	5.01	8.64	5.11	4.92
Share browsing history	2.99	4.67	3.01	2.70	4.84	4.25	3.75
Share voiceprint	3.37	1.32	4.78	4.60	4.12	3.18	3.56
Share info about your network	2.04	0.56	1.14	7.57	1.58	2.87	2.63
Share location	0.99	1.83	1.38	1.80	3.05	1.85	1.82
Send Ads	-0.29	0.27	-2.43	-0.95	1.83	1.14	-0.07

Calculations made using WTA estimates from Tables 2a-2d and the October purchasing power parity (PPP) conversion rates provided by the IMF. PPP conversion rates are: Argentina: 23.91, Brazil: 2.08, Colombia: 1340, Germany: 0.77, Mexico: 9.31.

Table 4: WTA Estimates for All Surveys in U.S. Dollars

		Argentina	Brazil	Colombia	Germany	Mexico	U.S.
Survey	**Feature**						
Carrier	Send Ads	0.65* (0.26)	0.84 (0.74)	-0.68* (0.34)	2.30** (0.40)	0.23 (0.34)	1.63** (0.40)
	Share location	1.84** (0.35)	2.88** (0.79)	2.51** (0.45)	3.51** (0.57)	3.84** (0.52)	2.50** (0.51)
	Share contacts	5.42** (0.59)	8.50** (1.59)	5.25** (0.69)	9.18** (1.12)	7.72** (0.81)	6.66** (1.13)
	Share browsing history	2.99** (0.39)	4.67** (1.08)	3.01** (0.56)	4.84** (0.65)	2.70** (0.43)	4.25** (0.76)
Financial	Send Ads	-0.74* (0.29)	0.01 (0.62)	-3.41** (0.83)	2.14** (0.56)	-0.90+ (0.48)	0.73** (0.25)
	Share balance	5.08** (0.57)	9.96** (2.00)	9.09** (1.82)	15.43** (2.57)	6.10** (0.95)	4.99** (0.79)
	Share cash withdrawals	3.66** (0.49)	4.88** (1.16)	6.72** (1.35)	13.42** (2.30)	3.12** (0.65)	3.03** (0.53)
Smartphone	Send Ads	-0.79** (0.30)	-0.04 (0.30)	-3.19** (0.65)	1.05** (0.34)	-2.18** (0.40)	1.06** (0.28)
	Share location	0.14 (0.32)	0.77* (0.39)	0.25 (0.62)	2.58** (0.40)	-0.24 (0.42)	1.20** (0.32)
	Share fingerprint	7.71** (0.85)	4.68** (0.66)	12.90** (1.63)	5.86** (0.77)	8.11** (0.98)	6.13** (0.88)
	Share voiceprint	3.37** (0.48)	1.32** (0.41)	4.78** (0.89)	4.12** (0.58)	4.60** (0.67)	3.18** (0.52)
Facebook	Read Texts	6.86** (0.70)	3.41** (0.50)	6.61** (0.65)	8.01** (1.88)	6.50** (0.73)	4.91** (0.84)
	Shares information about your network	2.04** (0.35)	0.56** (0.20)	1.14** (0.35)	7.57** (1.91)	1.58** (0.36)	2.87** (0.58)
	Share contacts	1.17** (0.30)	0.65* (0.30)	0.52+ (0.31)	8.09** (1.90)	2.30** (0.44)	3.55** (0.67)

Calculations made using WTA estimates from Tables 2a-2d and the October purchasing power parity (PPP) conversion rates provided by the IMF. PPP conversion rates are: Argentina: 23.91, Brazil: 2.08, Colombia: 1340, Germany: 0.77, Mexico: 9.31. Standard errors in parentheses. + is significant at 10% level. * is significant at 5% level. ** is significant at 1% level.

Table 5a: Coefficient of Variation Estimates for Carrier Survey

	Argentina	Brazil	Colombia	Germany	Mexico	U.S.
Send Ads	3.03** (0.61)	3.67** (1.33)	79.65 (426.29)	1.79** (0.25)	18.12 (20.66)	2.40** (0.32)
Share location	2.39** (0.37)	2.10** (0.37)	2.38** (0.37)	1.46** (0.17)	1.91** (0.22)	1.93** (0.24)
Share contacts	1.27** (0.09)	1.33** (0.09)	1.68** (0.21)	0.98** (0.10)	1.37** (0.11)	1.28** (0.10)
Share browsing history	1.60** (0.16)	1.74** (0.22)	2.27** (0.28)	1.20** (0.09)	1.99** (0.23)	1.43** (0.12)

All COVs reported as absolute values. Standard errors in parentheses. + is significant at 10% level. * is significant at 5% level. ** is significant at 1% level.

Table 5b: Coefficient of Variation Estimates for Financial Survey

	Argentina	Brazil	Colombia	Germany	Mexico	U.S.
Send Ads	7.25* (3.47)	6.60 (5.04)	2.85** (0.51)	2.07** (0.40)	8.07* (3.82)	3.43** (0.71)
Share balance	1.52** (0.12)	1.37** (0.10)	2.13** (0.25)	0.81** (0.06)	1.94** (0.21)	1.48** (0.10)
Share cash withdrawals	1.65** (0.14)	1.60** (0.16)	2.46** (0.38)	0.82** (0.09)	2.74** (0.41)	1.89** (0.17)

All COVs reported as absolute values. Standard errors in parentheses. + is significant at 10% level. * is significant at 5% level. ** is significant at 1% level.

Table 5c: Coefficient of Variation Estimates for Smartphone Survey

	Argentina	Brazil	Colombia	Germany	Mexico	U.S.
Send Ads	5.39** (2.02)	37.00 (92.49)	2.96** (0.63)	2.26** (0.35)	0.09 (0.655)	1.40** (0.33)
Share location	7.06* (3.24)	4.38** (1.28)	314.55 (5840.38)	1.58** (0.16)	10.37 (6.21)	2.31** (0.40)
Share fingerprint	1.18** (0.11)	1.70** (0.17)	1.27** (0.09)	1.14** (0.35)	1.35** (0.09)	1.20** (0.14)
Share voiceprint	1.48** (0.16)	3.19** (0.72)	2.45** (0.31)	1.24** (0.24)	1.72** (0.16)	1.47** (0.21)

All COVs reported as absolute values. Standard errors in parentheses. + is significant at 10% level. * is significant at 5% level. ** is significant at 1% level.

Table 5d: Coefficient of Variation Estimates for Facebook Survey

	Argentina	Brazil	Colombia	Germany	Mexico	U.S.
Read Texts	1.22** (0.07)	1.54** (0.14)	1.40** (0.10)	1.39** (0.13)	1.36** (0.10)	1.51** (0.13)
Shares information about your network	2.84** (0.42)	2.67** (0.51)	4.34** (0.98)	1.22** (0.10)	3.20** (0.52)	1.91** (0.22)
Share contacts	4.14** (0.83)	3.93** (1.07)	5.83* (1.57)	1.05** (0.07)	2.17** (0.23)	1.86** (0.21)

All COVs reported as absolute values. Standard errors in parentheses. + is significant at 10% level. * is significant at 5% level. ** is significant at 1% level.

Table 6a: Difference in WTA When Prompted for Carrier Survey

	Argentina	Brazil	Colombia	Germany	Mexico	U.S.
Send Ads	-1.78 (12.21)	-4.07 (3.40)	-496.43 (922.54)	-1.13 (0.72)	-5.47 (6.44)	0.05 (0.79)
Share location	-15.09 (16.81)	1.18 (3.22)	-542.05 (1241.84)	-1.23 (0.98)	3.54 (9.66)	0.44 (1.02)
Share contacts	30.21 (28.31)	-0.94 (6.63)	-2896.35 (1880.27)	-3.12 (1.96)	9.84 (15.14)	-0.57 (2.27)
Share browsing history	0.81 (18.64)	-0.75 (4.46)	1150.18 (1548.93)	-1.34 (1.10)	7.27 (8.00)	1.84 (1.52)

Units are in each country's currency. Standard errors in parentheses. + is significant at 10% level. * is significant at 5% level. ** is significant at 1% level. Note that Holm-adjusted p-value for Colombia is 0.35.

Table 6b: Difference in WTA When Prompted for Financial Survey

	Argentina	Brazil	Colombia	Germany	Mexico	U.S.
Send Ads	-8.40 (14.12)	4.73 (2.68)	-2818.07 (2159.10)	-0.25 (0.87)	6.33 (8.87)	0.08 (0.52)
Share balance	8.34 (27.41)	-0.29 (8.64)	-1269.47 (5049.41)	-3.64 (4.17)	23.24 (18.03)	2.67 (1.87)
Share cash withdrawals	-4.29 (23.47)	3.06 (4.85)	-3435.92 (3885.97)	-3.10 (3.69)	9.54 (12.20)	2.61+ (1.34)

Units are in each country's currency. Standard errors in parentheses. + is significant at 10% level. * is significant at 5% level. ** is significant at 1% level. Note that Holm-adjusted p-value for U.S. is 0.11.

Table 6c: Difference in WTA When Prompted for Smartphone Survey

	Argentina	Brazil	Colombia	Germany	Mexico	U.S.
Send Ads	-8.09 (14.27)	-0.52 (1.23)	1538.41 (1725.83)	-0.04 (0.52)	-16.52+ (8.49)	-0.64 (0.68)
Share location	2.81 (15.33)	-0.63 (2.73)	-573.87 (1689.72)	0.32 (0.61)	-1.52 (8.06)	-0.98 (0.80)
Share fingerprint	-8.86 (40.70)	-0.81 (1.68)	587.84 (4439.91)	-0.23 (1.19)	39.94* (20.28)	-4.72+ (2.62)
Share voiceprint	6.68 (22.78)	-0.29 (1.61)	1675.88 (2460.98)	0.38 (0.90)	22.87+ (13.62)	-3.27* (1.59)

Units are in each country's currency. Standard errors in parentheses. + is significant at 10% level. * is significant at 5% level. ** is significant at 1% level. Note that Holm-adjusted p-value for Germany is 0.09, for Mexico is 0.23, and for U.S. is 0.26.

Table 6d: Difference in WTA When Prompted for Facebook Survey

	Argentina	Brazil	Colombia	Germany	Mexico	U.S.
Read Texts	-54.24 (34.38)	-0.68 (2.06)	2934.08+ (1780.00)	-0.20 (2.90)	1.98 (13.57)	-1.67 (1.89)
Shares information about your network	-14.81 (17.19)	0.08 (0.83)	-397.80 (922.83)	-0.36 (2.94)	-5.03 (6.71)	-1.23 (1.31)
Share contacts	-21.35 (14.71)	-1.20 (1.21)	993.94 (828.23)	0.19 (2.92)	11.42 (8.27)	-1.04 (1.49)

Units are in each country's currency. Standard errors in parentheses. + is significant at 10% level. * is significant at 5% level. ** is significant at 1% level. Note that Holm-adjusted p-value for Colombia is 0.